"Cyber Crimes against Individuals in India and IT Act"

Introduction:-

Crime is a social and economic phenomenon and is as old as the human society. Crime is a legal concept and has the sanction of the law. Crime or an offence is "*a legal wrong that can be followed by criminal proceedings which may result into punishment."* The hallmark of criminality is that, it is breach of the criminal law. Per Lord Atkin "*the criminal quality of an act cannot be discovered by reference to any standard but one: is the act prohibited with penal consequences".*

A crime may be said to be any conduct accompanied by act or omission prohibited by law and consequential breach of which is visited by penal consequences.

The expanding reach of computers and the internet has made it easier for people to keep in touch across long distances and collaborate for purposes related to business, education and culture among others. However, the means that enable the free flow of information across borders also give rise to a worryingly high incidence of irresponsible behaviour. Any technology is capable of beneficial uses as well as misuse. It is the job of the legal system and regulatory agencies to keep pace with the same and ensure that newer technologies do not become tools of exploitation and harassment.

However, substantial legal questions have arisen in many contexts. The World Wide Web allows users to circulate content in the form of text, images, videos and sounds. Websites are created and updated for many useful purposes, but they can also be used to circulate offensive content such as pornography, hate speech and defamatory materials. In many cases, the intellectual property rights of authors and artists are violated through the unauthorized circulation of their works. There has also been an upsurge in instances of financial fraud and cheating in relation to commercial transactions conducted online.

The digital medium provides the convenient shield of anonymity and fake identities. Errant persons become more emboldened in their offensive behavior if they think that they will not face any consequences. In recent years, there have been numerous reports of internet users receiving unsolicited e-mails which often contains obscene language and amounts to harassment. Those who post personal information about themselves on job and marriage websites or social networking websites are often at the receiving end of 'cyber-stalking'. Women and minors who post their contact details become especially vulnerable since lumpen elements such as sex-offenders can use this information to target potential victims

Rationale and Significance of the Study

Humans are distinguished from other creatures by their technological initiative; in fact man has been described as a tool-using animal very often. History of human technology began with the how to give the stones cutting edge, and the discovery of fire, when compared with the level of technological knowhow common man today has, and how techno-savvy our life-styles has become we have come a long way. In today's age Information is said to be the currency which make the person successful in every aspect of his life. Technological marvels like the computers and the network systems have made possible a resourceful use of information. There is hardly

any facet of life that has not been touched by the information technology revolution, example, online banking, administration of justice, medical, education, agriculture travel etc, this piece of technology which is ever evolving has worked as a fountain of youth, an elixir of life for many with the only option that adaptation is the only mantra to survive and be successful.

The power of this technological advancement is such that the world has been shrunk into a global village with the introduction of tools like the Home PC, and the Internet as the information communications super-way. What is remarkably significant about this global village is that there are virtually no boundaries, and the distance between the places and people is reduced to a mere nothing. This feature has rapidly influenced the phenomenon of globalization, which has further have had a tremendous impact on the socio-economic and the cultural texture of the society. Thus the Information technology age has become a boon to the human community, but this paradigm-shrift in the human being all over is also reflected in the area of crime, as along with the positives there is a wide spectrum of negatives which has become a cause of worry because the negative facets are being efficiently utilized by the sadistic minds of the society for committing crimes in the virtual environment called the Cyber Crimes.

This newly emerging trend in the area of crime in the recent past was considered as a frontier zone not yet explored by any human soul has now started showing their physical features in the form of a multiple headed hydra, and it is becoming difficult to contain this threat through the agency of law. This is happening because the speed with which the society has adopted the technology in its mainstream of culture, it appears that the state which regulates the law through its agencies has been caught off–guard and seems to have failed to gain pace in order to catch up with the brilliant mind which are presently working to the detriment of the society at the moment.

Aims and Objectives of the Study

Any study is futile without a reasonable objective. The researcher believes that the increasing dominance and widespread scope of cyberspace and cybercrimes represents a major breakdown of International Law

Mankind has certainly come a long way and it goes unsaid that with progress come new challenges. The Information Technology Age which saw the unification of world in many ways, also saw the arrival of cyber specific legal challenges like data thefts, electronic frauds along with the arousal of contentious legal questions like who controls the cyberspace, where virtual players control and manage virtual property.

Also, with the absence of traditional barriers and due to the characteristics of cyber space like easier accessibility, anonymity and its superior reach the miscreants found the virtual world to be a perfect platform to wreak havoc; cyber pornography, defamation, IPR violations are some of the means being adopted by them with the most recent being cyber terrorism.

To tackle these complexities/problems of the virtual world separate legislations have been introduced in almost all countries along with the passing of certain universal codes like UNCITRAL laws. Thus we can see that the legal system of the physical world has been modified to accommodate the niceties of the virtual world.

This takes into account the above scenario and addresses issues like freedom of speech in cyberspace and data protection, vulnerability of e-commerce, IPR violations in cyberspace and most importantly the lacunae in the present Indian Law.

Scope of the Study

I take this opportunity to choose the topic **""Cyber Crimes against Individuals in India and IT Act""** Which have contributed to our Indian cyber laws? In particular to the cyber laws to curb the illegal use outstanding one of Information Technology laws.

Cyber Crimes against Individuals:

Against Individuals: –

- Harassment via e-mails

a) Email spoofing
(Online a method of sending e-mail using a false name or e-mail address to make it appear that the e-mail comes from somebody other than the true sender.)

b) Cyber pornography (exm.MMS)

- Cyber-stalking.
- Dissemination of obscene material.
- Defamation.
- Unauthorized control/access over computer system.
- Indecent exposure
- Email spoofing
- Cheating & Fraud Breach of Confidentiality

Computers as target of crimes: Due to the Home PC the use of computers has grown widely, such computers can become target of crime either in the physical or in the virtual manner, i.e. parts of the computer can be stolen example the hard disk thus leading to physical break-ins. Unauthorized access to the computer leading to confidential data loss will amount to virtual targeting of the computer, this will amount to a crime of data theft, which is termed as hacking in the ordinary parlance. Other forms of crimes in which the computer is the target include offences such as – Blackmail based on the information stolen in the form of medical information, personal data etc. this category can also include offences like the theft of Intellectual property, or important data of corporations like the marketing information etc. Further these crimes could also be committed with a mean intent by causing impediments in the business operation. Gaining access to the government records and making false passports, driver's licenses, manipulating the tax record, land record, accessing the intelligence files etc.

The type of victim's targeted also helps in establishing the typology of the Cyber crimes
Individuals: Most of the cyber crimes fall under this type, cyber staking is an example of an individual being affected through internet, or an individual may be affected even though he may have nothing to do with the cyberspace but still be victimized for instance online baking transaction frauds committed by hackers who gain entry into the computer systems of the banks.

National Security: E–mail as its is popularly referred to started becoming utilized for military applications. With the development of the World Wide Web this technology was inducted in the public domain. This is the starting point where the virtual medium started being utilized for criminal activities, and with the growth of terrorism, the terrorists also have adopted this technology. The terrorist's organizations all over the world have started using the internet to spread their ideology, and also for bringing in ability to their nefarious activities against any state or society at large. Further there are attempts done by terrorist organizations to disrupt the

communications hubs of the states, so that their activities could be carried with greater effect causing larger damage. In the context of national security, especially viz. military applications information plays a major role, on the basis of which military victories become decisive. This game of intelligence and counter-intelligence is carried out in the virtual medium as most of the military activities and the information management of most of the advanced nations is based on the use of computers and the internet. Thus disrupting the information's network of the advanced nations through the virtual medium has become a cost-effective technique resorted by the nation who do not have the military supremacy.

Economic crimes: This is one of the most widely committed crimes and with the society with every passing day more and more members of the society accepting e-commerce as a means to do commerce, crime through the virtual medium will be the one of the major dilemma which will necessarily be required to be contained through the agency of law. Major economic crimes under this classification are: Hacking, Virus, Cyber frauds, Software piracy and violation of copyrights, Industrial espionages by rival corporations Forgery and counterfeiting etc.

The content of the information also forms the basis for classification in deciding the typology of the Cyber Crimes –

The quantum of information being exchanged on the internet is beyond imagination. Not all the information being exchanged on the net has remained within the limits of public morality, thus the net has become a fertile ground for exchange of immoral information further leading to misuse of the right of freedom of speech and expression.

Cyber Pornography: This form includes act of publishing and printing pornographic material and the use of the internet to transmit such pornographic material. The Air Force Balbharti School New Delhi case is the first case to be registered in India u/s 67 of the IT Act 2000.

Propaganda of Racial and Hate Crimes: The internet is being used as a platform by terrorist groups for spreading their ideology instance of which are anti Jews groups, Muslim fundamentalists and such other groups have stated using internet for propagating violence against target groups.

The bottom line is that whatever may be the typology of the cyber crime may be the fact is that the virtual medium is being exploited by criminal minds for commission of crimes and such crimes are so innumerable in number that it has become impossible for the law enforcement agencies to keep a track of such crimes.

Society is dynamic; conventionally the law must match step with the steps of the society. However due to rapid technological advancements in communications and the computer technology have left the law trailing behind to such an extent that it is facing the complex challenges posed by the criminals of the new generation, who commit modern crimes with the help of technology.

The focal use of the net is to transfer files, exchange mails, for video conferencing, and the latest to add to these various purposes of communications is voice interface, these above mentioned forms of communications are carried out between the computer and a distantly accessible host computer, this form of communications becomes all the more important in the age where E–commerce has become a inevitable means of doing business.

Jurisdiction: Territorial limitation on the internet becomes of peripheral nature in the virtual medium as the web pages on the net can reach almost every province in the nation and conceivably almost every nation on the globe. This is where the point of friction between the cyber world and the territorial world begins as in the territorial world there are limitations set up by the sovereignty of the nation which is not the case in the cyber world.

A judicial system can function effectively if it is well regulated; it is these regulations that identify every functional aspect of the judicial system including the jurisdiction of the courts. A court in order to deliver effective judgments must have proper and well defined jurisdiction, as without a jurisdiction the court's judgments would be ineffective Jurisdictions are of two types namely, Personal and Subject Matter jurisdiction, and for a judgment to be effective both these types must exist contemporaneously. Further the conventional requirement as to a party can sue another is at the place where the defendant resides or where the cause of action arises. This itself is the problem with Internet jurisdiction as on the net it is difficult to establish the above two criteria's with certainty. Issues of this nature have contributed to the complete confusion and contradiction that plague judicial decisions in the area of Internet jurisdiction.

The IT Act 2000 passed in India is a perfect example of the ambiguous law in the area of jurisdiction in the context of the Internet. Section 1(2) provides that the act shall extend to the whole of India and, save as otherwise provided in this Act, it applies also to any offence or contravention there under committed outside India by any person. Similarly Section 75(2) provided that this Act shall apply to an offence or contravention committed outside India by any person if the act or conduct constituting the offence or contravention involves a computer, computer system or computer network located in India. Such a provision appears to against the principle of justice. Going to the next level, let's say even if the Indian court successfully assert jurisdiction and pass a judgment as per the above provisions of the IT Act 2000, the other question that arises will the foreign courts implement such a judgment? In case of the above predicament the only way to resolve such a dispute is by means of having an extradition treaty with the host nation and India, further it has been suggested by that the Indian court develop justifiable ground on which the extra-territorial jurisdiction may validly exercised as done by the American Judiciary[1].

From the above it becomes necessary to appreciate the complexities involved and thus it becomes indispensable to understand the nature of the Cyber crime, and whether the existing penal laws are sufficient.

When Macaulay came up with the Indian penal code in 1860 the notion of Cyber Crimes was completely unknown. Further until the IT Act 2000 was enacted there was no legal provision viz. Cyber Crimes; this was the sole rationale along with recognizing transactions carried on by means of electronic communications to augment the e-commerce, with which the IT Act 2000 was enacted. Further a blanket provision was made under section 77 of
the IT Act 2000 which provides that the penalties or confiscations provided under the IT Act 2000 will not release an offender from liability under any other law, in short the substantive provisions of the IPC are still applicable to Cyber Crimes committed in India[2].

[1]Nandan Kamath *'Law Relating to COMPUTERS, INTRENET AND E-COMMERCE'* pg 53

[2]**77. Penalties or confiscation not to interfere with other punishments:** No penalty imposed or confiscation made under this Act shall prevent the imposition of any other punishment to which the person affected thereby is liable under any other law for the time being in force.

Criminal Liability under Indian Criminal Law and the Information Technology Act 2000:The Indian Criminal Law hovers around the Indian Penal Code, tough there are other statutes which provide for criminal liability, but the Indian Penal Code is the sole authority in regards of deciding the conditions required of fulfill criminal liability. Various expressions have been used in defining offences under the Indian Penal Code like 'Intension', 'Knowledge' etc but in spite of this clinical treatment of mens Rea experience has shown that the court have imported the Common law maxim of mens Rea in the process of interpreting the offence defined under the Indian Penal Code and other special statutes[3]. Thus the Courts in India have been treating the concept of mens Rea on offence to offence basis. Thus it can be said that the maxim *"actus non facit reum nisi mens sit rea"* as a maxim has no significance to the offences under the Indian Penal Code. Where the code has not indicated any peculiar guilty intent or knowledge etc then the court presume, by considering the general definition that such an omission was made with some specific intention. In such case it would be unfair to import the maxim and arrive at a judgment declaring the offender guilty.

The Indian Law Commission in its 47th Report has mentioned that as a result of the transition process that the society was going through i.e. from a simple to an industrialized society it has become incumbent to contain the malpractices that were prevailing in the society then as such malpractices were unknown before for instance Unfair Trade Practices, Adulteration in Food, drugs etc, thus to restrain the emerging situation the judiciary and the parliament played a pivotal role in introducing the concept of Strict Liability because it is difficult to prove guilty intension of the offender in such socio–economic crimes. The effect of this was that with the imposition of Strict Liability under Criminal Law was that the burden of proof shifted from the prosecution to the defendant, and the Guilty mind need not be proved example in crimes like hacking it is almost impossible to prove guilty mind.

In regards of the Cyber Crimes under the Information Technology Act 2000 the Liability is divided into three categories. This has been done in order to avoid broad criminalization of all the wrongful acts in the virtual medium. Firstly there are certain wrongful acts that do not attract criminal liability and mens rea is not applicable to them, such acts are subject to civil penalties and strict liability is imposed on the wrongs of this category[4] e.g. failure to maintain books of accounts, or contaminating the computer with viruses etc. Secondly there are certain acts where mens rea has been made and fundamental part of the definition of the offence, thus expressions like 'Knowledge', 'intension' etc are included in the definition of such offences[5] e.g. tampering with the computer, publishing for fraudulent purposes etc. Lastly there are some acts or omissions that are made criminally liable with strict liability[6] e.g. Penalty for breach of confidentiality and privacy, penalty for misrepresentation etc

Antiquated Criminal Procedural Laws:

The distinctive feature of the cyber crimes has also had their consequence on the criminal procedural laws which have become more obvious in the areas of prosecution and investigation of the cyber crimes. The significant feature of this ever widening space between the law enforcement agencies and the cyber criminals is that the law enforcement agencies of most of the nations are not oriented for the dexterity necessary for investigating the crime in the virtual medium to add to this complexity is the trans-national nature of the cyber crime. The result is that

[3]' The Princes' Case 13Cox CC 138

[4] Sections 43,44,45 of the Information Technology Act 2000

[5] Sections 65,66, 67,74 of the Information Technology Act 2000

[6] Sections 71,72,73 of the Information Technology Act 2000

the traditional methods of crime investigation and the evidence collection have become obsolete partially. Following reasons can be attributed.

As per the traditional criminal procedure as soon as the police officer come to know about the commission of the offence he/she is expected to visit the scene of the crime, and collect the first hand details about the crime[7]. If the offence is of a cognizable nature then he must initiate investigation of the crime, but in case of a non–cognizable crime the officer is required to record the complaint and direct the informant to a Magistrate having power to try such case[8] The problem faced by the police officer is to begin with is that the victims are not aware of the fact that a crime has been committed against them or that the crime is being committed.

Further the police officer is empowered to ensure the attendance of the person who gives the information or who is acquainted with the facts and circumstance of the case. But in the context of cyber crime it has been noticed that there is very low reporting done of the crime to the police this factor must also take into consideration the non-realization of the commission of the crime. The reasons cited for the Non–reporting of the crime are many, and
many of them are of convincing nature e.g. fear of bad publicity, breach of security systems will affect the goodwill and confidence of the customers, fear of insurance cover of the companies been blown off, fear of transparency in the activities of the victim i.e. financial and other trade secrets will be required to be parted with to the investigation authorities etc.

Few steps[9] that have been recommended by Dr.S. V. Joga Rao in order to facilitate reporting and investigation of cyber crimes are:

- Establish an incident response policy.
- Maintain an up–to–date human resource record.
- Archive systems logs.

The next stage of investigation is of Search and Seizure by the Police officers and the collection of incriminating evidence connected with the crime. Again in the present context of cyber crimes the investigation process requires collection of the data, which further needs to be evaluated, which may be stored in a computer system located in some other country in case a of a trans-national computer crime. The police authorities find getting access to such data in other country difficult and time consuming. Further the investigation agencies need to be careful as the possible evidence in a computer system can be altered and the genuineness of such evidence is often challenged in the courts of law. The Indian Information Technology Act 2000 has addressed such issues by making amendments to the Indian Evidence Act 1872; the term electronic records have been included in the definition of the term evidence[10].

The Degree of power of search is also one important aspect which needs to be addressed. The problem mainly arises in the area of Public International law with respect to search and seizure of databases via an international telecommunications network systems, as any unauthorized penetration in such databases would amount to infringement of the sovereignty of that State where the data is stored, further such unauthorized access to any computer system is an offence in India[11]. Further the major hindrance that is caused in the investigation of cyber crimes is the level of expertise on the cyber forensics, as they must have extensive knowledge of the

[7] Sections 154,156, 157 of the Cr.PC
[8] Section 155 of the Cr.PC, committal of the case for trial
[9] Dr. S.V. Joga Rao *'Law of Cyber Crimes & Information Technology Law'* pg 194
[10] The Second Schedule of the Information Technology Act 2000 in Appendix.
[11] See Section 43 and Section 65 of the Information Technology Act 2000.

hardware, software, operating systems and the data-processing systems. Further the security software's, encryption software's limit the process of deciphering the data stored on the computer system. This is despite of the provision made in the criminal procedure code for the surrender of the documents or objects which are necessary for the investigation purpose either before the court or to the investigation officer on his written order[12]. Along with the above provision there is also a duty cast on the person in–charge of the premises to grant access to the investigation authorities[13]

Another aspect which needs to be highlighted in light of the search and seizure of data is the tapping of telephone communications lines. This becomes an inevitable necessity especially in the case of Internet crimes as data is only transmitted and not stored permanently on the computer system. This may necessitate real time monitoring system to make possible collection of evidence and make possible catching the suspect 'red handed'. But in order to make such provisions in law care need to be taken about the Right to privacy as unlike in the case of search and seizure, which amounts to perceptible interference which is of a limited nature, interception of the communication amount to gross invasion of the right to privacy. At the moment the power of wiretapping have been provided under section 5 of the Indian Telegraph Act 1885, which lays down a complex procedure and a so that this power is not misused. The Information Technology Act 2000 provided for a specific power to intercept transmitted information through any computer resource under section 69. Comprehensive provisions with detailed procedures were made in the Convergence Bill introduce in year 2000 viz. interception of all kinds of communication like wire, electronic communications etc, however this in due course lapsed and failed to become a law[14].

Cyber Crimes and the nature of Evidence:

The nature of evidence in the real world and the virtual world is different. This disparity is conspicuous in all the stages of evidence detection, gathering, storage and exhibition before the court. The critical part is that all the investigation authorities that are responsible right from the stage of collection of the evidence to the presentation of the evidence before the court must understand the distinguishing attributes of the evidence so that they can preserve the evidence collected by them. In this regard the role of the judiciary also becomes vital as the judiciary must also be in the position to appreciate the computer evidence presented before them. Contrary to the real world crimes where any tangible evidence in the form of finger prints, weapon of crime, blood stain marks etc can be traced, in the virtual world such traces become very difficult to find. The science of computer forensics is gaining significance in the investigation departments, corporate world, government departments etc. Let us understand some of the challenges that are involved in the process of cyber evidence detection, gathering, storage and exhibition before the court.

It is considered difficult to expunge the information from the computer system than what is generally contemplated. This can be done with the help of computer forensics who are able to gather evidence or even recover information which may have been deleted intentionally. It is vital that the victim report the law enforcement agencies about the crime as early as possible[15].

[12] See Section 91 of the Cr.PC
[13] See Section 100 of the Cr.PC
[14] Dr. S.V. Joga Rao *'Law of Cyber Crimes & Information Technology Law'* pg 182
[15] Supra, p16.

The process of preservation of cyber crime evidence lies within the understanding of an efficient and knowledgeable computer forensics expert because any carelessness in the process can lead to diminutive value of the evidence. The most often faced impediment is that the victim–companies are more concerned with restoration of their systems to full operational status rather than allowing proper evidence collection. Thus the timely assistance of the computer forensics expert can help collect evidence from the system within shortest time possible.

Cyber evidence is of physical or logical nature. It is the physical evidence that can be traced easily as the investigator just has to visit the scene of crime and search for and take into his custody computer hardware, which may constitute main frame computers to pocket sized personal assistants, floppy diskettes, electronic chips etc. The facets of the logical component of the cyber evidence are of different nature. This entails a process described as 'Information Discovery' wherein the investigator scrutinizes through the log files, and tries to salvage the data from a computer system which has been affected.

Once the required evidence is identified, then the investigator must ensure that the same is collected by adhering to the legal requirements, such as evidence is collected only after the requisite warrant for it is issued or if the information appears to be outside the scope of the warrant then additional warrant be issued. The evidence collected becomes valid in the courts of law only if the evidence is collected by legal means[16]. At the moment only officers not below the rank of a Deputy Superintendent of Police and officers deputed by the central government can be authorized to enter public places and collects evidence and carry out search operations and arrest[17]. This authority has been given to higher grade officers at the moment keeping in view the misuse of this power viz. right to privacy and ensuring the validity of the cyber evidence As of now in India the concept of 'Reasonable expectation of Privacy' has not be developed. The issues involved in this are that whether an 'individual's demeanor reflects subjective expectation of privacy' or 'the individual's subjective expectation of privacy is such that the society is ready to recognize it as reasonable'[18]

Another quarter which needs to be tested under cyber evidence and which is inevitable is the appreciation of the computer generated evidence by all the authorities associated with the process of administration of justice. Thus not just the judiciary[19] but also the prosecutors, the defence lawyers must become familiar with the technicalities, this is so because till now these authorities were dealing with evidence in the tangible form but the nature of evidence undergoes complete change under the virtual medium, they will have to adjust themselves to appreciate the evidence in logical format.

Conclusion:

Change is inevitable and the dilemmas that advancement in technology poses cannot be avoided, the truth is that the criminals have changed their method and have started relying of the advanced technology, and in order to deal with them the society the legal and law enforcement authorities, the private corporations and organizations will also have to change. Further such experts must not only be knowledgeable but must also be provided with necessary technical hardware and software so that they can efficiently fight the cyber criminals. Thus necessary

[16] Dr. S.V. Joga Rao *'Law of Cyber Crimes & Information Technology Law'* pg 197
[17] See Section 80 of the Information Technology Act 2000.
[18] Dr. S.V. Joga Rao *'Law of Cyber Crimes & Information Technology Law'* pg 198
[19] Section 46 of the Information Technology Act 2000 empowers the Central government in appointing adjudicating officers having experience both in the information technology and the legal field.

facilities must be established in various parts of the country so that crime in the virtual world can be contained[20].

Another aspect which needs to be highlighted is that a culture of continuous education and learning needs to be inculcated amongst the legal and the law enforcement authorities because the Information Technology field is a very dynamic field as the knowledge of today becomes obsolete in a very short time.

Lastly the preamble of the Information Technology Act 2000 provides that the act was passed with the objective to give legal recognition for transactions carried out by means of electronic data interchange and other means of e-commerce, further the act has also made amendments to the Indian Penal Code 1860, Indian Evidence Act 1872, The Bankers Books of Evidence Act 1891, and the Reserve Bank of India Act 1934 for facilitating legal recognition and regulation of the commercial activities. Though this objective of the act is not to suppress the criminal activity, this act has defined certain offences and penalties to smother such omissions, which is understood to come within the characterization of cyber crimes.

From this it can be inferred that the law cannot afford to be static, it has to change with the changing times and viz. cyber space this is all the more required, as there many application of the technology that can be used for the betterment of the mankind, similarly it equally true that such application can also be used for the detriment of the mankind as has been demonstrated by the Spy–cam case. The bottom–line is that the law should be made flexible so that it can easily adjust to the needs of the society and the technological development.

Following are some precautionary Measures to avoid Cyber Crimes against Individuals

- Cyber Forensics can be use to detect cyber Evidence
- To make necessary amendments in Indian laws to control on Cyber Crimes
- There is strong need to harmonize some sections of IT act 2000 to curb cyber crimes and Individuals to prevent cyber stalking avoid disclosing any information pertaining to one. This is as good as disclosing your identity to strangers in public place
- Always avoid sending any photograph online particularly to strangers and chat friends as there have been incidents of misuse of the photographs.
- Always use latest and up date anti virus software to guard against virus attacks.
- always keep back up volumes so that one may not suffer data loss in case of virus contamination
- Never send your credit card number to any site that is not secured, to guard against frauds.
- Always keep a watch on the sites that your children are accessing to prevent any kind of harassment or depravation in children.
- It is better to use a security programme that gives control over the cookies and send information back to the site as leaving the cookies unguarded might prove fatal.
- Web site owners should watch traffic and check any irregularity on the site. Putting host-based intrusion detection devices on servers may do this.
- web servers running public sites must be physically separate protected from internal corporate network

Bibliography:

[20] Cyber cell of the law enforcement agencies have started operating in metropolitan cities like Pune, Mumbai, Hyderabad, Chennai, Bangalore etc.

1. **Hand book of Cyber & E-Commerce – By P M Bakshi**
2. **Information Revolution in India – A Critique – By S S. Gill.**
3. **Computer Law – By Chris Reed & John Angle.**
4. **Indian Legislation on Cyber Crime – By S R. Sharma.**
5. **Cyber Crime Investigation Field Guide – By Bruce Middleton.**
6. **Cyber Crime – By R K. Suri. & T N. Chhabra.**
7. **Cyber Laws – By Justice Yatindra Singh.**
8. **Crimes in Cyber Space (Scams & Frauds) – By V D. Dudheja.**
9. **Intellectual Property - Cornish 3rd Volume**
10. **Computer & Cyber Laws - Nandan Kamath**
11. **Laws relating to Computers - Rahul Matthan**
12. **Indian Copyright Laws - Narayan**

Websites:

1. **www.benedict.com**
2. **www.UKPatentsandCopyrightOffice.com**
3. **www.kuesterlaw.com/kiprsrc.htm**
4. **www.co.broward.fl.us/lii12535.htm**
5. **www.llsdc.org/ip.htm**
6. **www.digmo.org/community/policy2.html**